25X1
25X1

23 March 1984

MEMORANDUM FOR: Director, Intelligence Community Staff
Executive Director
Deputy Director for Administration
General Counsel
Director, Office of Legislative Liaison

FROM: Director of Central Intelligence

SUBJECT: Intelligence Leaks and Counterterrorism Capabilities

1. We need a quick and intensive review of what could be done to attack the leak problem again in every possible way - legislatively, administratively, and every other conceivable way. The current staccato of leaks, the increasingly damaging impact and expression of concern and offers of support in the Congress mandate this. The latest and most shocking is the broadcasting

25X1

25X1
25X1

2. Particularly significant was Joe Biden's reaction - the tongue lashing he gave Justice for their passive attitude and general ineffectiveness, and his demand that, if the gray mail legislation which he sponsored was not enough to enable them to go after leaks, they tell them what else needs to be done. This all may make for an opportunity to launch a more effective campaign against leaking which can cost us the great bulk of intelligence assets if it keeps up.

3. I attach a memorandum prepared on how leaks damage our counterterrorism capabilities. The DDCI strongly disagrees with its passiveness and acceptance of our continued exposure to leaks even to the extent of seeing leaks as sometimes helpful.

4. Will all five of you get on this, working your respective areas of authority and influence, to gather ideas and do the necessary research to come up with a program of action.

5. I will meet with you whenever you are ready.

William J. Casey

225X1

Next 1 Page(s) In Document Denied

1h

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

Intelligence Leaks

FROM:
Harry E. Fitzwater
Deputy Director for Administration
7D-24 Headquarters

EXTENSION

NO.
OS 4 0731

DATE

25X1

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. D/Director of Central Intelligence				Hold for paper from ↑ Erase Done
2. DDCI	9 Apr.	9 APR 1984		
3.				
4. DDA				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

FORM 1-79 610 USE PREVIOUS EDITIONS

84-0975/

30 MAR 1984

STAT

MEMORANDUM FOR: Director of Central Intelligence

FROM: Harry E. Fitzwater
Deputy Director for Administration

SUBJECT: Intelligence Leaks

1. The epidemic of disclosures of classified information to the media continues unabated despite some conscientious efforts by the Executive Branch and the White House over the past three years to do something about the problem. Leaking is a growth industry. Leakers feel relatively safe in pursuing their selfish, sleazy, and furtive contacts with the media because experience shows that:

° Only a few agencies, e.g., CIA, NSA, act as if they really are concerned about the problem;

° There is a lot of apathy and fatalistic thinking about the leak problem in Washington;

° All of the agencies are devoting inadequate resources to the investigative and analytic efforts required in proper counterleak programming;

° The Department of Justice and the Federal Bureau of Investigation seem to feel that they have much bigger fish to fry than chase after leakers who probably won't be prosecuted anyway;

° Very few leak cases are solved and, when they are, the punishments tend to be mild--especially if the leaker is highly placed and has the right friends;

° The public is confused about the leak problem, thanks largely to the media, and tends to see counter-leak programming as attacks on the First Amendment or attacks on whistleblowers or as a smokescreen for corruption and inefficiency in the government.

STAT

2. The Willard Report which led to NSDD-84 was a noble try but it delivered a near disaster. The operation was a complete success but the patient died. Instead of helping with the leak problem, NSDD-84 was used by the media and its zealous supporters as a new weapon to beat on the very kind of programs--polygraph and prepublication reviews--that all the experts agree would help. The critics of the Willard Report won this battle and in doing so actually brought comfort to every government employee currently leaking classified information to the media. This battle was lost but the war goes on and it must be pursued with vigor and determination.

3. Although the record here is not perfect, this Agency's security program contains all the elements necessary for an effective defense system against unauthorized disclosures. It is a program worth promoting elsewhere in the Community. It's central features are:

° Careful security screening of all applicants for employment with all questionable cases decided in favor of the government;

° Comprehensive security review of all new employees within the first three years;

° Security reviews of all veteran employees every five years;

° Emphasis on security education and security awareness experiences for all employees throughout their careers;

° Security officers dedicated full-time to the investigation and analysis of leaks;

° Constant emphasis on protection of intelligence sources and methods;

° Use of the polygraph in both initial clearance-granting and in reinvestigation programming (This serves as a deterrent to leaking and occasionally helps solve a leak case.);

° A controlled system for media contacts, complete with a regulation on the books to enforce it;

° A system of penalties for violators of the regulations governing the protection of classified information;

° Actual execution of the penalties when appropriate;

° An effort to live by the "need to know" principle;

° A system of procedures that limit media persons' movements within Agency facilities, require certain official reporting on media contacts and force proper documentation of media contacts after the fact.

3. A multidimensional approach must be pursued to deal with the problem of leaks:

° Work with Intelligence Customers

--Require periodic rejustification of access to documents.

--Produce multiple formats and contents depending on customer needs.

--Require strict accounting, inventory and retrieval.

° Work with Automation Techniques

--Use computers more widely to track document deliveries, retrievals and distributions.

--Use computer technology more widely to effect audit trail production and analysis support.

° Work with the Directors of Security

--Seek dedicated people in all intelligence agencies to investigate all unauthorized disclosures.

--Seek standardization in leak investigative activity.

--Seek standardization in leak reporting and in damage assessment activity.

° Work with the Department of Justice and the Federal Bureau of Investigation

--Get a policy change that will have the effect of requiring DOJ/FBI investigation in all leak cases that are seen as damaging or threatening to intelligence sources and methods.

--Get a policy change that will discourage the DOJ/FBI from withdrawing from cases showing scant chance of prosecution or a large number of suspects.

--Work to get the Department of Justice and the Federal Bureau of Investigation more resources--perhaps dedicated units in each organization--to deal with leak investigations.

° Work with the Legislative Branch

--Seek a law which would make it a federal crime for a federal government employee and others with authorized access to make unauthorized disclosures of classified information.

--Get avenues built for legal relief that bypass the difficulties of dealing with the current espionage laws.

° Work with the Public

--Try to convince the public that leaks are harmful.

--Try to convince the public that the leaker is not a public-spirited whistleblower but rather a menace to the national security.

--Try to convince the public that counterleak programming is not threatening to the First Amendment nor to basic human freedoms.

Harry E. Fitzwater

Harry E. Fitzwater

Distribution:
Orig - Addressee
1 - ER
2 - DDA
1 - OS Registry
1 - D/Sec

STAT

SECRET

30 March 1984

25X1

MEMORANDUM FOR: Executive Director

FROM: James H. Taylor
Inspector General

SUBJECT: Intelligence Leaks

REFERENCE: Memo for Multi fr DCI, dtd 23 March 1984, Subj: Intelligence Leaks and Counterterrorism Capabilities

25X1

1. I have one thought on the subject of leaks which may not already have been expressed by the others asked to contribute ideas. Many of us are struck by the fact that our collective attitude towards secrecy and classification is very different from what it was ten years ago. Not long ago most Agency employees understood that everything we did was secret as far as the outside world was concerned--where we worked, who our coworkers were, what we did, how we felt about what we did, even what we thought about the events of the day. There didn't seem to be any gray areas. If you worked for CIA, everything about that relationship was considered classified, even when--strictly speaking--it wasn't. There wasn't much room for misunderstanding; the rules were very simple and easy to communicate

25X1

2. Today there is less certainty at all levels in the organization as to what is or is not appropriately shared with people outside CIA. Many of us seem to believe that we can be "more open" about what we can or can't discuss with acquaintances outside the Agency. The change in attitude reflects a number of developments over the past decade including these:

-- Much previously classified information became available to the public during the 1970's and continues to appear with excessive regularity in the media.

-- We continue to see examples of senior people who leave the Agency and seem able to publish a good deal about what they did when here.

All portions of this document are classified Secret.

25X1

SECRET

-- FOIA has contributed to a general impression that some of what we say or do here is unclassified.

-- Even the adoption of paragraph-by-paragraph classification has helped erode our previous sense that everything we did was confidential.

3. Just as important, I think we, as an Agency, have evolved a series of policies and attitudes that send mixed and possibly confusing signals to our employees about how we as an organization see our relationship to the world outside the Washington national security community. Witness our occasional tortured arguments about whether an Agency person should appear before this scholarly forum or that technical symposium. It may be irrelevant whether overall we are making consistently sensible decisions about the participation of Agency people in debates, media events, academic proceedings, or technical symposia. Rather, in approving "public" appearances and otherwise sometimes supporting our involvement in unclassified activities, we may be encouraging a general understanding that our employees can exercise their own judgment in deciding day-by-day what they can say to outsiders. (Probably very few mistakes are really made. But a few are too many.) In any event, despite some serious attempts to explain our views to our employees, I believe the distinction between what is classified and what is not, or what can be discussed and what cannot, is less clear than ever before. Does this "blurring" help establish a climate in which leaks become acceptable? I think that the answer to this has to be "to some degree, yes."

4. Certainly I wouldn't suggest that all the leaks around Washington are attributable to Agency people or practices. But it seems to me that the process of re-instilling some discipline in our government about the handling of classified information might begin with us. Maybe we can never get the various genies back in their bottles. But should not our primary goal be to recreate internally a broadly shared attitude that there is nothing about what we do which is an appropriate subject for discussion with people outside the building who lack the appropriate clearances? Clearly this could not be accomplished in a year or two; but I think it might be done in five. Where specifically would we begin? Probably we should start with some fact-gathering as to the nature and frequency of all relationships with the outside world (other than those which are 100 percent related to our work) by Agency employees. Excluded from any review would be such obvious activities as efforts to recruit assets, all authorized briefing activities, relationships with contractors where the relationship or product is classified, etc. Armed

SECRET

with a comprehensive understanding of the size and scope of the problem, we could change our policy and review procedures as appropriate.

5. Finally, I wish to comment on Stan Sporkin's suggestion that we find a way to hand over for investigation a leak case to some kind of unimpeachable outside expert such as a special prosecutor. It is true that there are many accusations that politics or preserving an Administration's reputation dictate our responses toward a specific leak problem. It is also true that probably neither we nor anyone else in Congress or the Executive Branch has the creditability that is necessary to address and satisfactorily resolve too many of the leak cases we see. There is, of course, a danger to adopting a "special prosecutor" approach. There will be cases--as there are now--where we will not be willing to share information with a special prosecutor. We will one day find ourselves in a situation where we can't satisfactorily explain why we are unwilling to take Case B forward when we yesterday pressed for a resolution of Case A. And given the perversity of the world, we will probably look like we're trying to cover something up when we find ourselves in that position.

25X1

James H. Taylor

Distribution:
Orig - Addressee
1 - ER
1 - OIG Subj
1 - IG Chrono
1 - Taylor Chrono

OIG/IG/JHTaylor/hr 30 March 84

SECRET

28 March 1984

MEMORANDUM FOR: Executive Director

FROM: George V. Lauder
Director, Public Affairs

SUBJECT: Director's Concern Regarding Intelligence Leaks and Counterterrorism Capabilities

REFERENCE: DCI's memo, this subject, dated 23 March 1984

1. If a new effort to stem leaks is to have any effect, we must first nail someone, or several people, under the Identities Act. It is the old story of hitting the donkey over the head with a two by four in order to get its attention. Efforts to educate people with access to classified information regarding the need to protect that information will only be effective after somebody has been prosecuted and convicted for leaking such data.

2. In order to prosecute successfully we have to get Justice's attention and cooperation. Since neither we nor the Congress have been very successful in that regard, perhaps we need to wheel the President himself, with the parallel cooperation of Congressional leaders, into the act to tell Justice to make a case, a good case, and see it all the way through. Stan Sporkin may have hit on the right avenue for proceeding, i.e., a special prosecutor or investigator. I recommend retired Supreme Court Justice Potter Stewart as the right person to head such an inquiry. He has the right national stature, integrity and attitude. When he was on the PBS series "the Media and National Security", he said "there is nothing in the Constitution about the public's right to know."

3. Then we need to go for legislation for criminal sanctions for unauthorized disclosures of classified information. Other than the Espionage and Identities Acts, Comint law, and firing people, there are no enforceable penalties for leaks that I know of. People feel free to leak since they are risking little.

4. Resources in the Intelligence Community agencies, especially Defense, State and the FBI, are woefully inadequate to cope with the number and difficulty in investigating the spate of leaks which have been occurring. Their resources should be greatly augmented and devoted exclusively to pursuing leak investigations.

5. Defense and State and the Oversight Committees should develop educational programs and reports to promote understanding among their officials as to the truly damaging effects leaks can have on very important

national security programs. We keep seeing in the press that, according to Congressional testimony, leaks aren't a problem. Six identified leaks were reported during the year, etc., etc. We need to get the story out through the Oversight Committees, if possible, about the true figures and that the damage caused is clearly serious.

6. Last, we need to continue our efforts to educate the media regarding the need to protect sources and methods (I have worked hard on this and with some success) and to educate the other Public Affairs Officers in the Community to emulate the Agency's efforts to better control media contacts with their officers and other employees.

STAT

George V. Lauder

Distribution:
Orig - Addressee
1 - ER
1 - PAO #84-0148
2 - PAO files
1 - C/CCIS

STAT